Requester Name:	- Review of Garda National Data Protection Unit		File FOI- 000131-2021		
Page No	**Description of Document**	**Deletions**	**Relevant Section of FOI Acts**	**Reason for Redaction**	**Decision Maker's Decision**
1	Cover Page	1	Part 1(n) of Schedule 1	Out of Scope	Part-Grant
2	Table of Contents	0			Grant
3-4	Executive Summary	2	Part 1(n) of Schedule 1	Out of Scope	Part-Grant
5	Terms of Reference	1	Part 1(n) of Schedule 1	Out of Scope	Part-Grant
6-23	Detailed Findings & Recommendations	33	Part 1(n) of Schedule 1, Section 37	Out of Scope, Personal Information	Part-Grant
24-25	Appendices	2	Part 1(n) of Schedule 1	Out of Scope	Refused

Audit Report

Review of Garda National Data Protection Unit

Date Issued: 28/02/2022

[redacted]

GARDA INTERNAL AUDIT SERVICE

Table of Contents

1. Executive Summary

An Garda Síochána became subject to the provisions of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) on 25th May 2018, and the Garda National Data Protection Unit (GNDPU) was established in 2018. When processing personal data for law enforcement purposes, An Garda Síochána is subject to the provisions of Part 5 of the Data Protection Act 2018, which transposed the Law Enforcement Directive (LED, EU 2016/680) into national law. Processing for other purposes is carried out under the GDPR.

Both the LED and GDPR significantly expanded upon the existing rights of data subjects and the responsibilities of data controllers such as An Garda Síochána when processing personal data. Under data protection legislation data controllers must appoint a Data Protection Officer (DPO) to inform and advise the controller and the employees of the controller of their obligations under data protection legislation.

In July 2019 the Policing Authority approved 17 new posts in the Data Protection Unit (DPU) to support the newly appointed DPO. The Data Protection Unit's functions include:

- Managing subject access requests (SARs) on behalf of An Garda Síochána (approximately 7,000 requests per annum, of which approximately 500 per annum involve requests for specific personal data such as witness statements, personnel files or CCTV footage);
- Liaison with the Data Protection Commission (DPC) on complaint cases lodged by data subjects, data breaches, investigations, audits and inquiries;
- Assistance to other business areas in An Garda Síochána to investigate and address instances of data breaches;
- Assistance and advice to other business areas in An Garda Síochána with data protection queries, including the development of data sharing agreements with data controllers and data processors;
- Assistance and advice to other business areas in An Garda Síochána with conducting Data Protection Impact Assessments (DPIAs), including management of the consultation processes with the DPC where required under legislation or recommended by the DPO;
- Data protection policy development, and engagement with business areas across An Garda Síochána to raise awareness and provide training;
- Evaluations and audits to assess compliance of individual business areas with data protection legislation and identify and address issues.

1.1 Summary of Findings

The audit findings are detailed in the main body of this report and key findings are summarised below.

[redacted]

- GNDPU currently has no portal page to provide data protection information within the organisation.
- The DPO has informed GIAS that he does not have adequate resources to perform his functions, as required under the Data Protection Act 2018.
- No comprehensive data protection training has been provided to all employees in the wider organisation.

[redacted]

1.2 Audit Assurance Level

The overall assessment of the control environment is considered by the auditors to be 'Limited' due to the lack of relevant data protection policies and the lack of internal support available and public information provided.

	Potentially Systemic	Applicable to Location Audited	Total
High	4	0	4
Medium	2	0	2
Low	0	0	0
Total	**6**	**0**	**6**

1.3 Acknowledgements and Limitations

Garda Internal Audit Service (GIAS) would like to thank management in the GNDPU for all their assistance throughout the course of this audit.

The contents of this report should be considered in the context of the following:

- Findings are based on information provided by the GNDPU.
- The findings and associated risks identified are not exhaustive and no assurance is provided that additional risks do not exist.
- Findings are based on point in time review for the year 2021.

2. Terms of Reference

2.1 Audit Objective

This audit aims to review progress on the establishment of the GNDPU, evaluate the adequacy of resourcing and training of staff in the unit to perform its functions and provide adequate support to An Garda Síochána with data protection issues and compliance.

2.2 Audit Scope and Methodology

This audit is an 'as is' examination of progress on the establishment of the Garda National Data Protection Unit (GNDPU).

GIAS examined the following areas

- Adequacy of staffing resources:
- Structure of the Unit:
- Training:
- Functions:
- Engagement with the organisation and its stakeholders

GIAS interviewed management and examined the processes and controls in place for completing the unit's functions. This was conducted through walkthroughs examining subject area requests, data breaches, complaints and CCTV redactions. GIAS also reviewed documentation provided by the management of GNDPU.

The audit also examined the unit's capacity to provide adequate support to An Garda Síochána to inform and advise employees of their obligations under data protection legislation.

2.3 Reporting Arrangements

3. Detailed Findings and Recommendations

Listed hereunder are all the key audit findings, implications and recommendations together with a time schedule for the implementation of the recommendations.

Findings	Risk / Potential Implication	Recommendations	Management Comment
1. Data Protection Legislation and Policy			**High (S)**
The processing of personal data by An Garda Síochána is governed by data protection legislation. Where processing takes place for law enforcement purposes (such as preventing or detecting crime) the 'Law Enforcement Directive' (LED) covers these situations, the rules for which are found mainly in Part 5 of the Data Protection Act 2018 (which implements the LED into Irish law). GNDPU has responsibility for data protection policy development, and engagement with business areas across An Garda Síochána to raise awareness and provide training in terms of compliance with data protection laws. The following gaps in policy have been identified as required to inform Garda personnel of their obligations under data protection legislation: • Data Management Policy • Data Classification Policy • Records Management Policy • Records Retention Policy	The absence of up to date policies, procedures and guidance to employees of An Garda Síochána will increase the risk of data breaches, complaints, fines and sanctions. [redacted]	GNDPU should develop a strategy that includes details of its responsibilities and objectives, and the resources, including staff, required to satisfactorily achieve those objectives. [redacted] GNDPU should initiate a communications programme that aims to disseminate relevant data protection policies and procedures throughout the organisation.	**Management Comment:** The gaps in policy referenced in the findings in this section are derived from a business case developed by the [redacted] DPO in early 2021 and approved by the Garda Executive in June 2021. [redacted] [redacted] Colleagues in GIAS rightly identify the risks the current policy gaps present to the organisation in respect of breaches, complaints, fines and sanctions. In line with the first recommendation by GIAS, the business case outlined the Data Protection Unit (DPU)'s responsibilities within the context of the wider Garda National Data Protection Office (GNDPO, encapsulating DPU and FOI and headed by the DPO), and the additional resource requirements needed to:

Findings	Risk / Potential Implication	Recommendations	Management Comment
			• Establish DPU's Policy, Audit and Compliance functions; • Increase DPU's resources for managing Specifics requests (in particular those involving multimedia which are complex and resource intensive to process); and, • Progress a suite of wider Data and Records management policies (those policies referenced in the findings column) for the organisation through the establishment of a new Office of the Chief Records Officer (OCRO), separate to DPU and within the overarching GNDPO. Since its establishment, the DPU has necessarily prioritised managing mandatory requirements under data protection legislation on behalf of AGS, with resources prioritised to manage subject access requests, personal data breaches, and liaison with the Data Protection Commission (DPC) on DPC inquiries and audits and to progress and resolve complaints by data subjects. The initial staffing compliment was designed in effect to centralise and inherit data protection responsibilities from other business areas based on the requirements of

Findings	Risk / Potential Implication	Recommendations	Management Comment
			the previous legislative regime, without factoring in the increased requirements of the LED and GDPR. In spite of this resourcing gap, some limited policy initiatives have been progressed by the DPU (for example [redacted] which provides advice on a key topic of requests for personal data from third party data controllers). In respect of a measure to '*inform Garda personnel of their obligations under data personnel of their obligations under data protection legislation*' as outlined in the findings, the primary outstanding requirement to be progressed by DPU is to develop an updated Data Protection Code of Practice for An Garda Síochána. [redacted] Within its current resources and capacity, DPU has continued to provide bespoke advice, guidance

Findings	Risk / Potential Implication	Recommendations	Management Comment
			and training on data protection issues to colleagues across the organisation, but by necessity on a mostly reactive basis. [redacted] [redacted] Dedicated resources for this work is required to assist AGS in meeting its obligations as a data controller. For DSAs the need for dedicated resource is particularly acute in the context of new requirements for data sharing agreements between public sector bodies that will be introduced with the scheduled commencement of the Data Sharing and Governance Act 2019. [redacted] [redacted]

Findings	Risk / Potential Implication	Recommendations	Management Comment
			Following the Executive approval of the business case in June 2021, both the AGS Chief Information Officer and AGS DPO have been liaising with colleagues in HR for updates on the progress of the case. The last update received was that the business case is currently with DPER for consideration. **Responsible Person:** Once sanction of the business case is received, the **AGS DPO – Michael Armstrong** will take primary responsibility for liaison with HR to ensure the resourcing requirements needed to make progress on GIAS's second and third recommendations are addressed as a priority. **Implementation Date:** Assuming sanction of the business case is received and DPU's policy, audit and compliance function can be adequately staffed by **June 2022** (see Finding 3), development and approval of an updated Data Protection Code of Practice and associated communications plan could be progressed and completed by **December 2022**.

Findings	Risk / Potential Implication	Recommendations	Management Comment
2. Engagement			**High (S)**
Under data protection legislation data controllers must appoint a Data Protection Officer (DPO) to inform and advise the controller and the employees of the controller of their obligations under data protection legislation. In addition, Section 88(4)(d)(i) of the Data Protection Act 2018, the Data Controller shall also support the DPO by providing him or her with the resources that he or she requires to perform those functions. GNDPU currently has no portal page providing data protection information internally to employees.	Limited engagement with the organisation to raise awareness of the functions of the unit will lead to a lack of employee awareness of their responsibilities under GDPR regulations. This may result in data breaches, data breaches not being reported, complaints and fines or sanctions to the organisation.	GNDPU should develop a portal page to provide information to all employees about their responsibilities in relation to GDPR and the data protection laws, policies, procedures and internal guidance notes.	**Management Comment:** The response to Finding 1 above outlined the resource needs identified by the [redacted] DPO, which were considered and endorsed by the Garda Executive in June 2021. Sanction of the associated business case is awaited. In respect of the specific recommendation regarding a portal page, this can be progressed to provide general advice and guidance on AGS's responsibilities similar to the content already available on the Garda website (https://www.garda.ie/en/information-centre/data-protection/) and outlined in the Data Protection aide memoire displayed to all users at log in to any Garda computer. This portal page, once established can be further updated as policy and training initiatives/topics are progressed, including the updated Code of Practice detailed under Finding 1. [redacted]

Findings	Risk / Potential Implication	Recommendations	Management Comment
			[redacted] **Responsible Person:** The [redacted] **Head of DPU, Liam Behan** will take responsibility for establishing the DPU's portal page. **Implementation Date:** Portal page to be established by **April 2022.**

Findings	Risk / Potential Implication	Recommendations	Management Comment
3. Resources			**High (S)**
There are currently 18 members of staff appointed to the unit. Eight trained staff have left the unit within the last three years and five Clerical Officers were retained by the Garda National Vetting Bureau for other functions. A business case for additional staff was approved by the Garda Executive in June 2021. This has been submitted to the Policing Authority and approval is currently under consideration. [redacted] As per the Data Protection Act 2018, the Data Controller should support the Data Protection Officer in performing his function by providing him with the required resources. The DPO has informed GIAS that he does not have adequate resources to perform his functions.	Noncompliance with data protection legislation due to lack of human resources will increase the risk of complaints and possible sanctions due to best practice not being followed. Inadequate service delivery due to lack of resources and high turnover of trained staff.	GNDPU should have adequate staff resources to achieve its objectives. [redacted]	**Management Comment:** The response to Finding 1 above outlined the resource needs identified by the [redacted] DPO, which were considered and endorsed by the Garda Executive in June 2021. Sanction of the associated business case is awaited. The business case outlined a range of functions within the unit that currently lack dedicated resources. As identified by colleagues in GIAS, DPU's delivery of its core functions has also been impacted by high levels of turnover within DPU's currently sanctioned staffing levels. This included turnover of senior staff, with the DPO (PO), Head of Unit (AP), and Deputy Head of Unit (HEO) initially appointed when the unit was established all transferring out of the unit between 2019 and 2021. Key factors contributing to staff turnover include the availability of secondments and/or mobility opportunities that are more attractive for career development or in terms of work/life balance (e.g. reduced commuting times). A further internal factor is the lack of available progression routes for staff

Findings	Risk / Potential Implication	Recommendations	Management Comment
			to be retained within DPU on promotion, or capacity within the unit to cycle staff between processing of requests and more varied development opportunities related to policy, audit and compliance issues. Sanction of the business case, once received, should provide more opportunities to retain staff with specialist knowledge and training on data protection issues, however the delays in receiving sanction have most recently prevented retention of the unit's most experienced Specifics request manager (EO) on promotion to HEO. [redacted] bringing the total turnover of staff since 2018 to 9. [redacted]

Findings	Risk / Potential Implication	Recommendations	Management Comment
			Responsible Person: In line with Finding 1, once sanction of the business case is received, the **AGS DPO – Michael Armstrong** will take primary responsibility for liaison with HR to ensure the resourcing requirements needed to make progress on GIAS's recommendations are addressed as a priority. **Implementation Date:** Assuming sanction of the business case is received in the coming weeks, the target date for addressing DPU's resource requirements is **June 2022**

Findings	Risk / Potential Implication	Recommendations	Management Comment
4. Training			**Medium (S)**
GNDPU has responsibility for data protection policy development, and engagement with business areas across An Garda Síochána to raise awareness and provide training in terms of compliance with data protection laws. A presentation has been added on the Learning Management System (LMS) for APs, Superintendents, HEOs and Inspectors as part of their respective development courses. No comprehensive training has been provided to other ranks/grades on their responsibilities in terms of data protection laws.	A lack of knowledge by AGS staff of their data protection responsibilities due to inadequate training by GNDPU leads to data breaches and non-adherence to statutory obligations within AGS	Develop a training programme that suits AGS's unique data protection requirements and ensure a planned roll out of the training across the organisation is commenced.	**Management Comment:** Prior to the onset of COVID-19 and the move to remote working, the AGS DPO and Head of Unit provided onsite training and presentations to business areas, with a particular focus on regular presentations on data protection and FOI provided as part of the Inspector development course. As outlined in GIAS's findings, the AGS DPO developed and recorded an e-learning package with the Garda college that provides an overview of key concepts and requirements of data protection legislation. While initially recorded for the Senior Management Development Programme, the college has since incorporated the training into the HEO and Inspector development programme and has been requested to consider mainstreaming the e-learning package for a wider range of roles/grades. [redacted]

Findings	Risk / Potential Implication	Recommendations	Management Comment
			[redacted] **Responsible Person:** **AGS DPO – Michael Armstrong** will liaise further with the Garda College [redacted] **Implementation Date:** **September 2022**, factoring in the potential need to design and record grade/rank specific packages with the Garda College [redacted]

Findings	Risk / Potential Implication	Recommendations	Management Comment
5. Secific Subject Access Requests			**Medium (S)**
Under Articles 15 – 22 of the GDPR when a valid Subject Access Request (SAR) is received by AGS they must respond to the request without undue delay and at the latest within one month of receiving the request. GNDPU can extend the time to respond by a further two months if the request is complex. These are called Specific Subject Access Request (SAR). Specific requests can include requests requiring a large volume of paper documentation (e.g. personnel records) but can also relate to multimedia requests which involves the redaction of CCTV footage to be reviewed for disclosure [redacted]	[redacted]	An assessment should be undertaken of GNDPU's staffing, training, hardware and software needs in order for GNDPU to fulfil statutory requirements.	**Management Comment:** The responses to Findings 1 and 3 refer in respect of the resource needs identified by the [redacted] DPO, which were considered and endorsed by the Garda Executive in June 2021. Sanction of the associated business case is awaited. In tandem training requirements for the unit have been identified and highlighted in returns to the Garda College, with relevant external training secured as the opportunities for same have arisen. [redacted]

Findings	Risk / Potential Implication	Recommendations	Management Comment
			[redacted]

Findings	Risk / Potential Implication	Recommendations	Management Comment
			[redacted]

Findings	Risk / Potential Implication	Recommendations	Management Comment
6. AGS and Data Protection			**High (S)**
The Eight Principle of the Future of Policing in Ireland report from 2018 by the Commission on the Future of Policing in Ireland states that policing must be information led, and the AGS Corporate Strategy 2019 – 2021 stated that the organisation will rebuild confidence in our data through accurate recording and governance. The Garda Code of Ethics commits Garda personnel to gather, retain, access, disclose or process information in accordance with the law and principles of data protection. The 2020 Policing Plan and related Key Performance Indicators, which were reported on in the 2020 Annual Report Policing Plan published by AGS in October 2021, and the 2021 and 2022 Policing Plans do not outline annual data governance or data protection objectives. The Garda website contains a Data Protection page, which includes information on data protection rights, contact details for the DPO and data protection requests. No information is provided in relation to AGS's data protection policies.	[redacted]	[redacted]	**Management Comment:** The page on the Garda website referenced by colleagues in GIAS (https://www.garda.ie/en/information-centre/data-protection/) provides information on the right of access and how to contact the AGS DPO as outlined in the findings. It also satisfies information requirements detailed under data protection legislation in outlining the purposes for AGS's processing of personal data, and the applicable legislative regimes that apply to this processing. A detailed breakdown of data subject's rights in addition to access is provided, as is AGS's general approach to data sharing and the contact details for the Data Protection Commission (DPC) as the relevant supervisory authority with oversight of An Garda Síochána's processing of personal data. [redacted]

Findings	Risk / Potential Implication	Recommendations	Management Comment
			[redacted]

Findings	Risk / Potential Implication	Recommendations	Management Comment
			Responsible Person: **AGS DPO – Michael Armstrong**